OPSWAT.

DATASHEET

Filescan Sandbox

Advanced Threat Analysis Platform

OPSWAT Filescan Sandbox platform combines static and dynamic analysis with machine learning powered threat intelligence for highly accurate and rapid malware analysis. Our platform can analyze 25K+ files per day per machine. Enhance defensive capabilities, save time, and effectively hunt threats with advanced threat analysis.

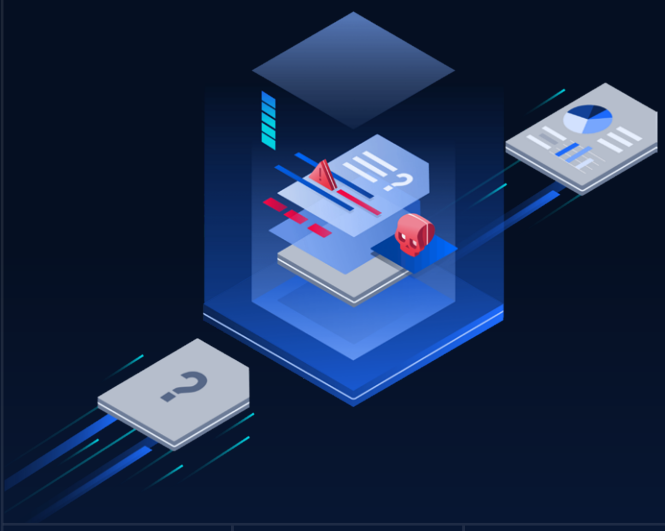
Overview

- Static analysis uses 30+ antivirus engines, Yara rules, and threat patterns for high-volume processing.
- Dynamic analysis virtually detonates malware with adaptive threat analysis to expose highly evasive malware and zero-day threats.
- Threat analysis accesses 50 billion+ hashes, IPS and domains, and includes threat actor attribution.
- ChatGPT executive summary generator.

Traditional Sandbox

Slow	High resource use	Detectable

Emulation Sandbox



Fast	Small Memory Footprint	Adapts to multiple environments

Platform Features

Stage 1

Deep Structure Analysis

Initial static file assessment and extract embedded active content.

- Analyze 50+ different file types
- Extract artifacts, images, and more
- Automated decoding, decompilation, & shell code emulation
- Extract and decode scripts and macros

Stage 2

Threat Detection and Classification

Detect and classify threats using machine learning and decades of experience.

- Detect 290+ brands for ML-based phishing detection
- Extract and correlate a wide range of IOCs
- Detect malicious intent with 400+ generic behavior indicators
- ML-based similarity search detects unknown threats and malicious clusters

Stage 3

Adaptive Threat Analysis

Perform dynamic analysis on active content using adaptive threat analysis. Detect and classify threats using machine learning and decades of experience.

- Detonate targeted attacks via specific application stacks or environments
- Bypass a wide range of anti-evasion checks
- Emulate JavaScript, VBS, PowerShell scripts
- Automatically adapt the control flow

Stage 4

Threat Intelligence and Automation

Perform automated threat hunting and real-time threat identification using a wide range of integrations.

- Export to MISP & STIX report formats
- Query MD Cloud reputation service
- Integrate with other open-source intelligence vendors
- Automatically generate YARA rules on a per threat basis

Integrations

OPSWAT

- MetaDefender Core
- MetaDefender Cloud
- Threat Intelligence Search API

SOAR

- Splunk SOAR
- Palo Alto XSOAR
- Assemblyline 4

Others

- Virus Total
- Python CLI

- CEF Syslog Feedback
- Chrome Extension
- Passive Email Analysis
- OpenAPI Specification (OAS)

Flexible Deployments

On-Premises

- Intel Xeon-E 2136 (12M Cache, 3.30 GHz)
- RAM 32GB DDR4 ECC 2666 MHz
- 2x SSD NVMe 256GB RAID

Note: example system processes 25K files/ day with a retention period of 10 days.

Cloud

- 5000 scans/day: t3a.2xlarge
- 10000 scans/day: c4.4xlarge
- 25000 scans/day: c4.8xlarge

Read minimal requirements here.

OPSWAT.

Protecting the World's Critical Infrastructure

OPSWAT.com/contact